

Implementing CD Copyright Protection by Using TCPA Framework

by

Nurashikin Mohd. Hussin

Dissertation submitted in partial fulfilment of
the requirements for the
Bachelor of Technology (Hons)
(Information Technology)

DECEMBER 2005

Universiti Teknologi PETRONAS
Bandar Seri Iskandar
31750 Tronoh
Perak Darul Ridzuan

CERTIFICATION OF APPROVAL

Implementing CD Copyright Protection by Using TCPA Framework

by

Nurashikin Mohd. Hussin

A project dissertation submitted to the

Information Technology Programme

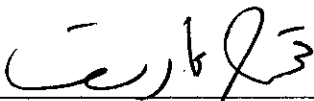
Universiti Teknologi PETRONAS

In partial fulfillment of the requirements for the

BACHELOR OF TECHNOLOGY (Hons)

(INFORMATION TECHNOLOGY)

Approved by,



(Mrs. Mazeyanti Mohd. Ariffin)

UNIVERSITI TEKNOLOGI PETRONAS

TRONOH, PERAK

December 2005

CERTIFICATION OF ORIGINALITY

This is to certify that I am responsible for the work submitted in this project, that the original work is my own except as specified in the references and acknowledgements, and that the original work contained herein have not been undertaken or done by unspecified sources or persons.



NURASHIKIN MOHD. HUSSIN

ABSTRACT

The main objective of this research is to study the current issue of the copyright protection behind the music and software industry. The study also propose a protecting mechanism of commercial audio CDs and software in order to reduce the number of unauthorized duplication of the CDs by consumer. Currently, the music and software industry is facing the piracy problem. This issue is getting bigger from time to time. Therefore, this research will be focusing on current copyright issue, preventing method by using trusted computing framework, TCPA.

In developing the project, the research procedures being taken by the author are observation where the author figures out the broad problem area of the research, followed by preliminary data investigation and problem definition. The next phase is data collection, analysis and interpretation, and also report writing. The last two phases are the development phase and report and project presentation phase. Meanwhile, the author discusses about findings gathered through out this research. The end product of this research is the concept of how TCPA can be implemented in protecting the copyright of the CDs and also the simulation demo authored in Java. The simulation will demonstrate the action taken by CPU in handling CD.

ACKNOWLEDGEMENT

First and foremost, thanks to the Lord Almighty for given me strength, wisdom and patience to complete the Final Year Project.

As a most gracious mentor and guide, I would like to thank my supervisor, Mrs. Mazeyanti Mohd Ariffin for introducing me with the concept of TCPA and also for the tremendous support and guidance throughout the period. It is with your patience and understanding made me achieve the objectives meant to at the conception of this project. I hope the experience during the development of this project will be beneficial, and bring warm and sweet memories during the years to come.

Also not forgetting, to express my gratitude to my family. Without their financial and emotional support I may not be here today. Thank you and love goes to Ayah and Mama for the encouragement, trust and joy you have allowed me during my stay at UTP. Same goes to my brothers, Napie, Wan and Anip. Thank you for the countless and meaningful advice and *doa* for me.

Sincere thanks to my wonderful friends Suriana Jumali, Wirdhayu Mohd Wahid, Wan Norazlinawati Wan Abd Arif, Julia Hazleen Rostam, Nuraimi Saari and other close friends for giving hope to carry on this project whenever I felt like giving up on the project. Wish you all the best. May our journey be worth all the laughter and tears.

Last but not least, sincerely thanks to individuals who have helped me in this project even though I have not mentioned their names.

TABLE OF CONTENTS

CERTIFICATION		i
ABSTRACT		iii
ACKNOWLEDGEMENT		iv
CHAPTER 1:	INTRODUCTION	1
	1.1 Background of study	1
	1.2 Problem statement	3
	1.2.1 Problem identification	3
	1.2.2 Significant of project	4
	1.3 Objectives and scope of study.	5
	1.3.1 The relevancy of the project	5
	1.3.2 Feasibility of project within scope and time frame	6
CHAPTER 2:	LITERATURE REVIEW AND THEORY	7
CHAPTER 3:	METHODOLOGY / PROJECT WORK	10
	3.1 Research procedures	10
	3.1.1 Observation	11
	3.1.2 Preliminary Data Investigation	12
	3.1.3 Problem Definition	12
	3.1.4 Data Collection, Analysis and Interpretation	13
	3.1.5 Report Writing	14
	3.1.6 Development	14
	3.1.7 Report and Project Presentation	16

CHAPTER 4:	RESULT AND DISCUSSION	. . .	17
	4.1 Result	. . .	17
	4.1.1 Finding	. . .	17
	4.1.2 Flow of the Simulation	. . .	18
	4.1.3 Interface of the Prototype	. . .	19
	4.2 Discussion	. . .	23
	4.2.1 Copyright Protection	. . .	23
	4.2.2 Copyright Protection by Implementing TCPA		25
CHAPTER 4:	CONCLUSION AND RECOMMENDATION	. . .	27
	5.1 Conclusion	. . .	27
	5.2 Recommendation	. . .	28
REFERENCES		29
APPENDICES		30

LIST OF FIGURES

- Figure 3.1 Research Procedures
- Figure 3.2 Data Analysis and Interpretation
- Figure 3.3 Simulation of CD Copyright Protection
- Figure 4.1 Flow of the Simulation
- Figure 4.2 Interface of the Simulation
- Figure 4.3 Interface of the Simulation
- Figure 4.4 Interface of the Simulation
- Figure 4.5 Interface of the Simulation
- Figure 4.6 Interface of the Simulation
- Figure 4.7 Interface of the Simulation
- Figure 4.8 Interface of the Simulation
- Figure 4.9 Interface of the Simulation
- Figure 4.10 Interface of the Simulation

ABBREVIATIONS AND NOMENCLATURES

<i>BSA</i>	Business Software Alliance
<i>CD</i>	Compact Disc
<i>CD-R</i>	Compact Disc-Recordable
<i>CD-ROM</i>	Compact Disc-Read Only Memory
<i>CPU</i>	Control Processing Unit
<i>ECC</i>	Error Correcting Code
<i>HMAC</i>	Hashing for Message Authentication Calculator
<i>P2P</i>	Peer to peer
<i>PCR</i>	Platform Configuration Register
<i>R&D</i>	Research and Development
<i>RNG</i>	Random Number Generator
<i>RID</i>	Recorder Unique Identifier
<i>TC</i>	Trusted Computing
<i>TCPA</i>	Trusted Computing Platform Alliance
<i>TPM</i>	Trusted Platform Module

CHAPTER 1

INTRODUCTION

1.1. Background of study

Copyright protection or also known as copy prevention, is any technical measure designed to prevent duplication of information. The goal is not to make it impossible to copy, but rather to discourage casual copying of software and music. The media industries have always referred the technology as copy protection. The term is often related and/or confused to the concept of digital rights management. Digital rights management is a more general term as it includes all sort of management of works, including copy restrictions, nevertheless copy protection may include measures that are not digital.

Copyright protection is commonly found on videotapes, DVDs, computer software disc, video game discs and cartridges, and more recently on some audio CDs. A more recent innovation is copyright protection for audio CDs, inspired by the rise of MP3 trading over the Internet. This is more difficult to do, because the protection must allow correct behavior on a CD player but altered playback when being read by a CD-ROM drive. The best that can be accomplished is to force the user to play the music in an analog format and then re-digitize it, resulting in an imperfect reproduction.

A separate but related issue is “counterfeit protection”, where the publisher wants to make it easy to detect mass-produced duplicates. As for example, Microsoft’s placement of the holograms on the hubs of their CD-ROMs.

Some people have questioned whether copy protection is legal. In some countries it may not be. However, the law allows “fair use” of copyrighted material, but it does not mean that the content provider can make it easy for user to do so. So while making a copy of a song as a user private use may be legal, there is nothing in the law that requires the publisher to make material available in an unprotected format. Copyright protection has been around for many years, some of the schemes employed on the Apple II were remarkably elaborate and has never been challenged on legal principle.

Therefore, in this research, the author attempts to study the current issue of copyright infringement and figure out possible solution to overcome the problem.

1.2. Problem statement

1.2.1. Problem identification

Copyright infringement or often referred to as piracy or theft (an early reference was made by Alfred Tennyson in the preface to his poem "The Lover's Tale" in 1879), poses a greater threat to the international music and software industry than at any other time in its history. The piracy not only growing globally, but it is rapidly diversifying into new technologies and formats.

As for the music industry, the commercial CDs copyright infringement today range from the traditional cassette to the manufactured CD, and from the CD-R disc replicated in a garage or laboratory to the audio file distributed on the Internet. Adding the threat to the copyright infringement of commercialized CDs is the spread of CD burning, which make it possible by any advances in digital copying technologies. The global pirate music market totaled 1.8 billion units in 2000, meaning that more than one third of CDs and cassettes around the globe are illegally produced and sold. Worldwide sales of pressed pirate CDs were 475 million units, up from 450 million in 1999, and the sales kept increasing in 2000, from US\$ 4.1 billion in 1999 to US\$ 4.2 billion. This situation will affect the revenues for both artists and record companies, where only about 16% of CDs sold make enough money for the publishers to break even. As for the recording artists, only about 3% sell enough music to get any royalties. With figures like these, it's not surprising that the industry is taking steps to combat piracy.

Lately, the business software industry feels like a bit of music industry war on piracy. "We tend to have gotten a little bit lost in the shuffle," said Bob Kruger, vice president of enforcement for the Business Software Alliance (BSA). According study conducted by BSA, four in 10 software products are illegally copied worldwide. On average, the software industry loses about US\$11 to US\$12 billion in revenue to software piracy annually. Of the billions of dollars lost to piracy, a little less than half comes from Asia,

where China and Indonesia are the biggest offenders. Piracy is also a big problem in Western Europe, where piracy losses annually range from \$2.5 and \$3 billion dollars. Piracy rates are quite high in Latin America and in Central Europe, but their software markets are so much smaller that the dollar losses are considerably lower.

Piracy has changed the landscape of today digital culture drastically. Peer to peer (P2P) file sharing technology and IRC have allowed for the easy spread of not only pirated software and audio CDs, but also massive amounts of information. Safeguarding the content and software is often a mandatory part of the music and software publishing industry.

There is no doubt that there several copy prevention techniques available in the market. Most companies who are affected by the piracy have believed that copy protection will increase the company's revenues, by limiting the ability of the consumer to make copies of the CD's contents. As in the absence of copy protection, most of the CDs are relatively easy to copy in their entirety using a machine. Copy protections used currently are far from effective and can easily be bypassed.

1.2.2. Significant of project

It is significant to have a protection on CDs copyright. By having protecting mechanism on the CDs, the copyright infringement can be prevented. There is critical need in figure out corrective measure in preventing unauthorized duplication of CD contents. The prevention measure being taken not only protecting the contents and respecting people's intellectual property right, but may also improve the civic engagement. Moreover, by preventing piracy, the economies can be stimulated as if the piracy drop to 30%, economic growth could increase by \$400 billion and it would create 1.5 million jobs and generate \$64 billion in taxes. The proposed solution will not eliminate piracy completely

(likely an impossible task), rather the goal should be to make participation in widespread infringement unattractive, risky and rare.

1.3. Objectives and scope of study

The objectives of the study are as listed below;

- To study the implementation of TCPA in CD copyright protection
- To provide solution that can discourage copying
- To prevent unauthorized duplication of commercially purchased audio CDs and software.

The scope of this study emphasizes on copyright infringement issue and how to prevent the unauthorized copying of commercial CD and software. The main highlight of this study is the attempt to create a simulation, acting as a mechanism that preventing the user from copying the content of CD illegally. This study also outline the framework to be used in protecting the copyright in a manner that is consistent of current technology trend.

1.3.1. The relevancy of the project

With referring to the objectives defined for the study, it is hoped that this study would benefit not only to music and software industry itself, but also the consumers. The author would like to promote civic engagement among the users, to show them to be more respectful to others work. Moreover, this project may also help in introducing the trusted computing framework. As nowadays with the current widespread of high end technology, the project should not encounter any difficulties.

1.3.2. Feasibility of project within the scope and time frame

It has been stated that the project must be completed within 14 weeks, or roughly in 4 months. With this allocated time frame, it should be enough for the author to conduct research based on the scope of study. The project objectives and functional requirements will be the basis for the project to be developed. Moreover, a Gantt chart will be created to organize the time frame effectively.

CHAPTER 2

LITERATURE REVIEW AND THEORY

2. LITERATURE REVIEW AND THEORY

According to Wikipedia glossary, a copyright is a set of exclusive rights granted by government for a limited time to regulate the use of a particular form, way or manner in which an idea or information is expressed. Copyright may subsist in a wide range of creative or artistic forms or "works". These include literary works, movies, musical works, sound recordings, paintings, photographs, software, and industrial designs. Copyright is a type of intellectual property.

The first copyright dispute occurred around 560 between Saint Columba and Saint Finnian when Columba secretly copied a psalter Finnian possessed after being granted permission to look at it. The origins of copyright systems are generally placed in practice of various monarchs in granting letter patent, arbitrary grants of monopoly over a particular practice or trade. Such grants were an invaluable source of power for rulers who possessed much theoretical authority, but little cash. In the two centuries following the invention of the printing press, such grants were given periodically to printers (and occasionally authors) with regard to particular works. In Britain, the culmination of this practice was the Licensing Act of 1662, which granted a monopoly on the entirety of English publishing to the Stationers' Company of London (the *quid pro quo* for this grant was censorship of heretical and seditious material). The Stationer's company had developed its own inter-publisher system for regulating competition, now known as *Stationer's copyright*, which was effectively a private copyright system made enforceable by the Stationers' monopoly (Lowenstein, 2002).

All software comes with a license agreement that specifically states the terms and conditions under which the software may be legally used. Licenses vary from program to program and may authorize as few as one computer or individual to use the software or as many as several hundred network users to share the application across the system. It is important to read and understand the license accompanying the application to ensure that you have enough legal copies of the software for your organization's needs. Making additional copies, or loading the software onto more than one machine, may violate the copyright law and be considered piracy (The Software & Information Industry Association).

Lessig mentioned that the Internet has unleashed an extraordinary possibility for many to participate in the process of building and cultivating a culture that reaches far beyond local boundaries. That power has changed the marketplace for making and cultivating culture generally, and that change in turn threatens established content industries. Thus, on the surface copyright infringement of CD content looks like a simple crime of stealing another person's or company's information or material. Piracy is not merely about the illegal sharing of software or protection of personal property, there is more at stake when it comes to the freedom to share all information without restrictions.

The threat of piracy seems to grow greater by the day. Just walk into any *pasar malam* and witness the large number of makeshift stores selling illegal copies of songs, and movies. In addition, there is the new frontier, cyber piracy. With broadband Internet connectivity so prevalent and accessible these days, anyone can easily download, for free almost any movie, and song. It is a problem that takes millions of ringgit away from musicians, producers and the rest of the entertainment and software industry that supports these people. Naturally, it warrants greater attention from those working in the industry to make the local entertainment industry successful.

While major international software companies bear the brunt of piracy losses in the country, the phenomenon also acts as a disincentive for the development of homegrown software companies. Piracy is pulling the plug on a potentially lucrative local software industry. A quick check of a few software companies listed in Mesdaq within the last two years shows that these companies allocated up to 48% of proceeds from their public issues as funds for R&D. The recording industry loses some RM16bil worldwide every year, according to the Recording Industry Association of America. That's a small loss compared with the RM110bil in global losses for software piracy in 2003. Losses in Malaysia due to software piracy came up to about RM490mil. Every ringgit lost represents theft from the local economies where software products are made and sold. Not only do governments lose sales and corporate taxes, but piracy costs jobs – those of software company workers *and* the jobs created when those workers spend money (Ong, 2005).

The Software & Information Industry Association has stated using pirated software is risky for all users. Aside from legal consequences of using pirated software, the organization forfeits some practical benefits as well. Those who use pirated software:

- increase the chances that the software will not function correctly or will fail completely;
- forfeit access to customer support, upgrades, technical documentation, training, and bug fixes;
- have no warranty to protect themselves;
- increase their risks of exposure to a debilitating virus that can destroy valuable data;
- may find that the software is actually an outdated version, a beta (test) version, or a nonfunctioning copy;
- are subject to significant fines for copyright infringement; and
- risk potential negative publicity public and private embarrassment.

CHAPTER 3

METHODOLOGY / PROJECT WORK

3.1. Research Procedures

Research may be defined as a process being undertaken within a framework of a set of philosophies and designed to be unbiased and objective. Research procedures which is the way where data are collected for the research project is important to be clarified. Although research does not necessary have to solve problems, it may also equipping oneself with additional knowledge. Therefore, research plays a significant role in this project, not only to highlight issue related to CD copyright protection and TCPA, but also to enhance the knowledge of the author.

In completing this project, the procedures used can be defined as below;

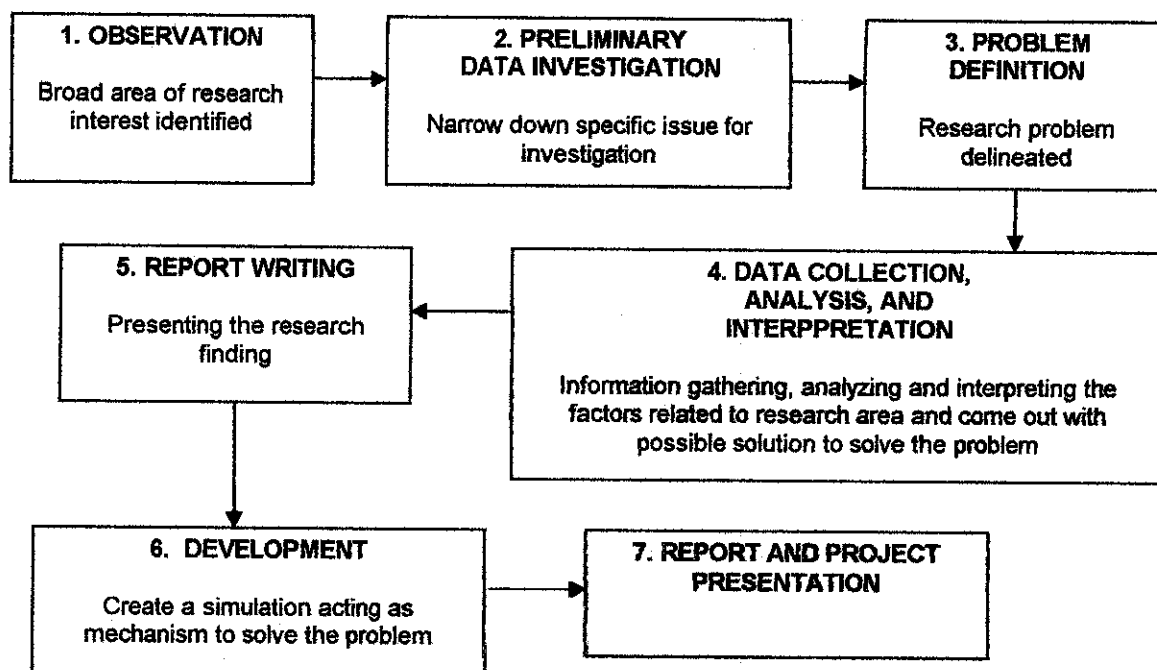


Figure 3.1 Research Procedures

3.1.1. Observation

In observation phase, the broad problem area is being identified through out the process of observing and focusing on the situation. The broad area problem refers to the entire situation where a possible need for research and problem solving can easily being identified. Along the observation phase, understanding the requirements of this Final Year Project course is very important. The main things to be highlighted basically how will the research being conducted, on what area the research is all about, the time frame and also the expected final result. Through out the discussion with the supervisor, the author has decided to focus on security and copyright protection as the research area.

3.1.2. Preliminary Data Investigation

In order to figure out specific scope for the research area, preliminary data investigation is being conducted in the second phase. The preliminary data investigation is conducted by having literature survey. The documentation of a comprehensive review of the published and unpublished work from secondary sources of data in the areas of specific interests may help in narrowing down the broad problem area. In conducting the literature survey, the first step involved in this phase is identifying the various published and unpublished materials that are available on the topic of interest, and gaining access to these materials. The next step would be gathering the relevant information by going through the necessary materials in library and Internet. Lastly, the third step is writing up the literature review based on the information gathered. The author gathered as much as possible information regarding security and copyright protection as a reference in delineating the research problem.

3.1.3. Problem Definition

After the literature review, the next phase is narrowing down the problem from its original broad base and defines the issues of concern more clearly. Identifying the focus of the research or problem is important. Based on the observation and preliminary data investigation, the author identified issues related with the security. Current technology in the security area being discussed is the Trusted Computing Platform Alliance (TCPA). The theory behind TCPA framework is quite interesting. The TCPA can be implemented in copyright protection. In narrowing down the scope, the author focuses on piracy issue within music and software industries. Even though the author realises that the available techniques in CD copyright protection, however, those techniques does not prevent piracy as the pirates still can make copies from the protected CDs. Therefore, all the way through discussion, the topic choosen for this research is 'Implementing CD Copyright

Protection by Using TCPA'. Once the topic has being choosen, the next steps is identified the goals and objectives of this research, scope of study and time estimated to conduct the research.

3.1.4. Data Collection, Analysis and Interpretation

Data is gathered from published and unpublished materials such as newspaper, magazines, and Internet. Furthermore, data also gathered all the way through discussion with the supervisor.

In data analysis and interpretation, steps has being taken is shown in Figure 3.2 below;

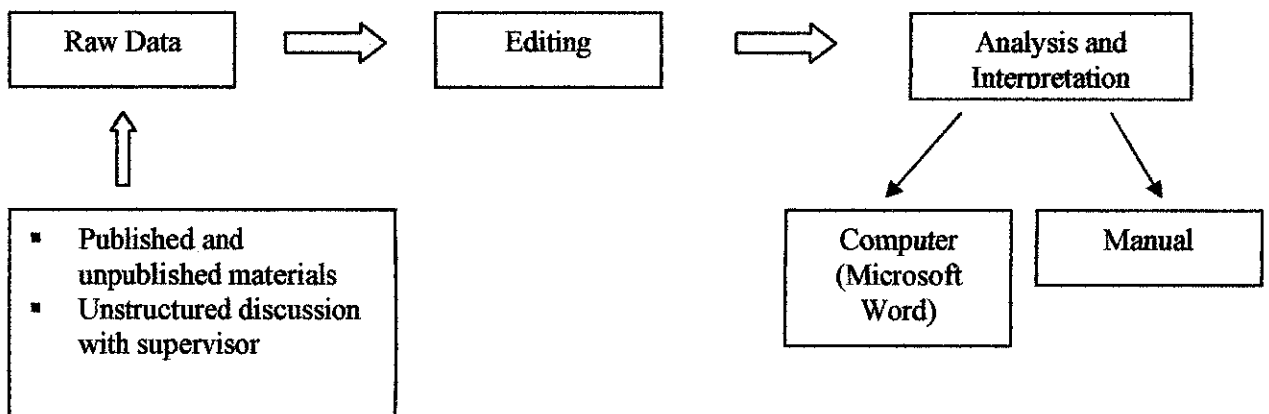


Figure 3.2 Data Analysis and Interpretation

3.1.5. Report Writing

From time to time, all findings during conducted this research will be written up. This report will be updating phase by phase with the assisted of the Supervisor. The final report will document overall findings and result of this research.

3.1.6. Development

In development phase, the first task to be encountered is to draw the flow of the simulation and also define tools to be used, goals and constraints of the simulation. Later, all aspects are defined in details and serve as the system specification. System specification is one of the main features that should be identified in achieving the project objectives. Yet, the main task is developing this simulation to come out with function calculating hash value. The process of coding the hash function algorithm is the critical part in developing this simulation. Hash function algorithm will be used to encrypt the serial number of a specific CPU. The hash function or also know as digest function is a one way function that easy to calculate, however it is hard to invert. The hash function algorithm is compatible with the C, C++ and Java language. As for this project, the Java language has been selected. The details coding of hash function library class can be referred in Appendix.

Once the coding of hash function algorithm has being finalized, the next step is creating the interface of the simulation. The programming tools has being choosen is the Java version J2SDK 1.4.2_03. The simulation consists of three parts; the first part demonstrates a CD being inserted for the first time and action taken by the CPU, the second part describe action taken by the CPU if the hash value of serial number contains in the CD does not match with the hash value of serial number of the CPU, and lastly the third part illustrates what will happen if both hash value in CD and CPU match to each

other. The theory behind this simulation is based on the concept of TCPA (Trusted Computing Platform Alliance) framework. TCPA is a family of open specifications whose stated goal is to make personal computer more secure through the use of dedicated hardware. The basic system concepts of the trusted computing are:

- unique identification using certificates stored inside the computer's chip
- all encryption is performed in the hardware
- data can be signed with the chip's identification
- data can be encrypted with the chip's secret key

The final step in the development phase is to integrate the hash function library class created earlier with the simulation. The interface of the simulation is as shown in Figure 3.3 below;

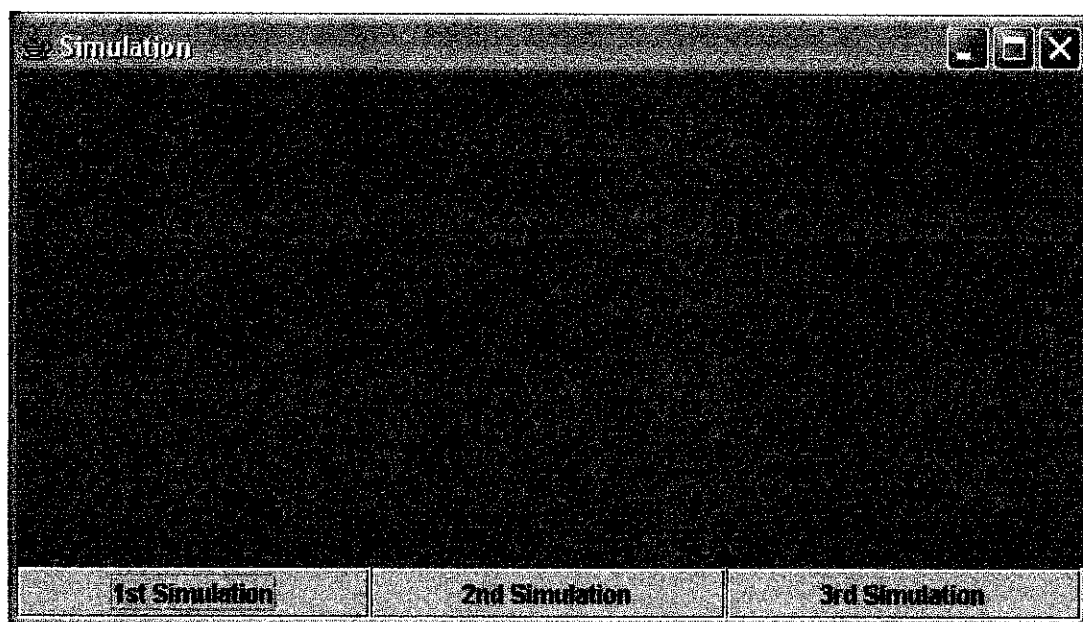


Figure 3.3 Simulation of CD Copyright Protection

Even though this research involved simple simulation and report writing, there are few commercially available software being used. Java version J2SDK 1.4.2_03 are used to produce the simulation while Microsoft Office Word 2003 is needed to produce the report. However, there is no specific hardware needed along conducting this research.

3.1.7. Report and Project Presentation

Based on the research procedures, the final task is presenting the report and project. The report and project is being presented to the respective supervisor, and also to both internal and external examiners.

CHAPTER 4

RESULT AND DISCUSSION

4.1. RESULT

4.1.1. Finding

From the research that has been conducted, there is possibility to implement TCPA in protecting the copyright of CD. Meaning to say that, the TCPA can be used to protect the contents of the CDs from being copied by unauthorized parties. As the version 1.0 of TCPA chip was published in 2000, and the TCPA chip is available in market since May 2002 where the user is able to install it in the IBM ThinkPad series of laptop. Moreover, some of existing features in Windows XP are TCPA features; for example if a user attempted to change PC configuration more than a little, the user have to re-register all the software with Redmond. Also, since Windows 2000, Microsoft has been working on certifying all device drivers, whereby if user tries to load an unsigned driver, XP will complain. The Enterprise Rights Management stuff is shipping with Window Server 2003. Moreover, TC developers' kits are available in October 2003.

As the development in TCPA is rolling from time to time, the author seems that implementing TCPA in CD copyright protection is achievable.

4.1.2. Flow of the Simulation

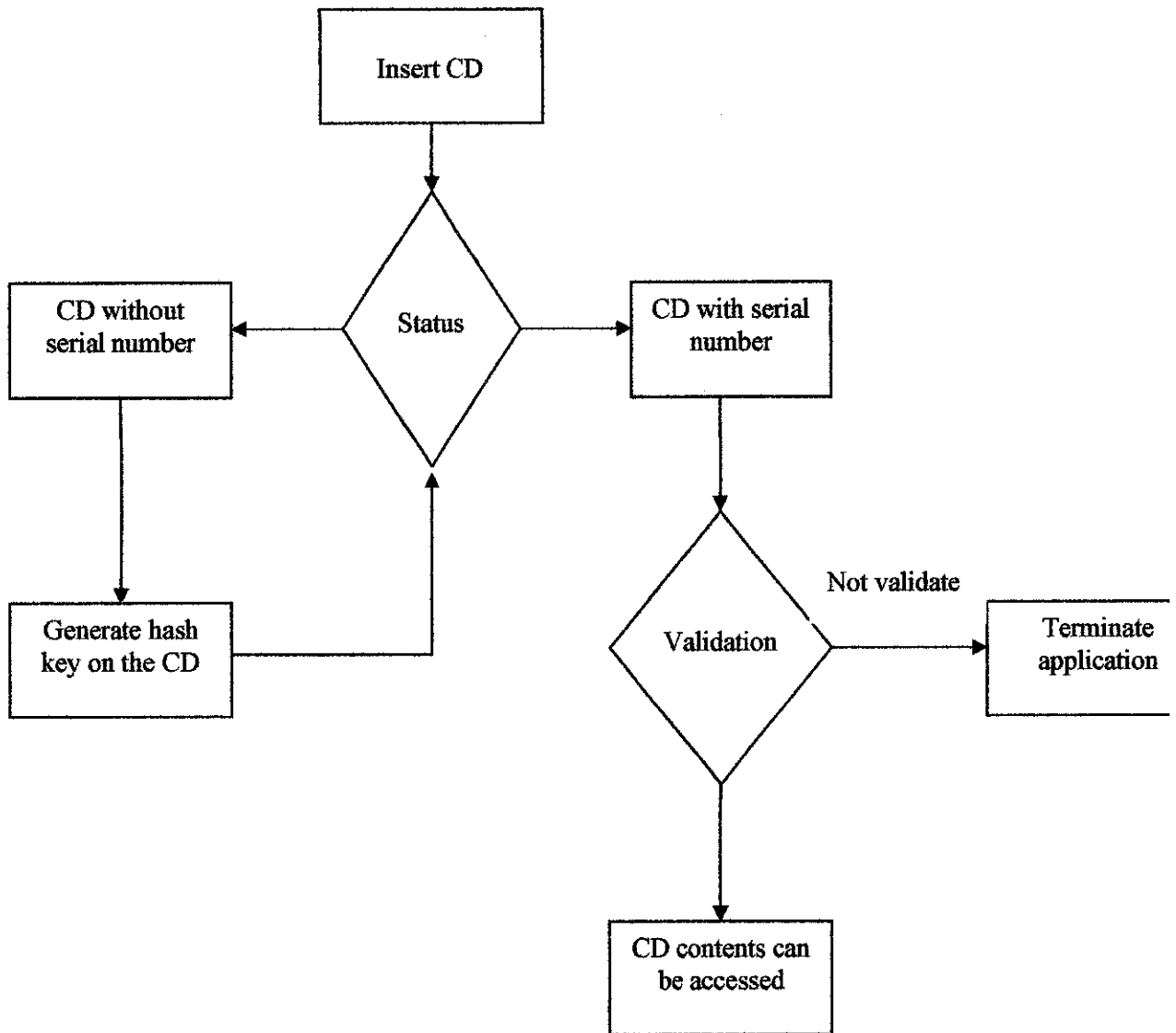


Figure 4.1 Flow of the Simulation

Figure 4.1 above describe the flow of the simulation. First, as CD being inserted into CPU, the status of the CD will be checked, either the CD is having hash value of serial number or not. If the CD does not have any hash value, it will denote that the CD is being inserted for the first time. Therefore, the CPU will hash its serial number and burned the hash value into the CD. On the other hand, if the CD has come with a serial number, the CPU will validate the hash value. If the hash value matches with the hash value of the CPU's serial number, then the CD contents can be accessed. However, if the hash value does not match, the application will be terminated.

4.1.3. Interface of the Prototype

Basically, the first part of the simulation illustrates a new CD, either audio or software CD being inserted for the first time. The simulation is shown as stated below;

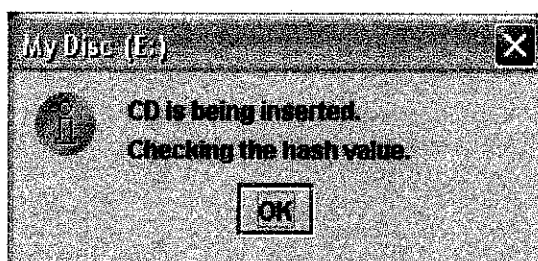


Figure 4.2

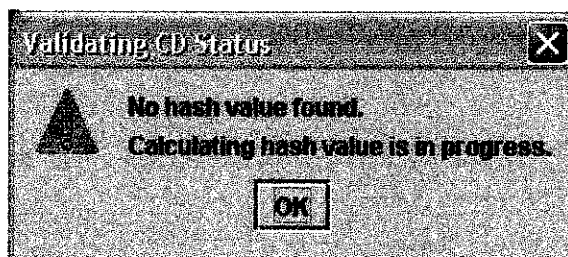


Figure 4.3

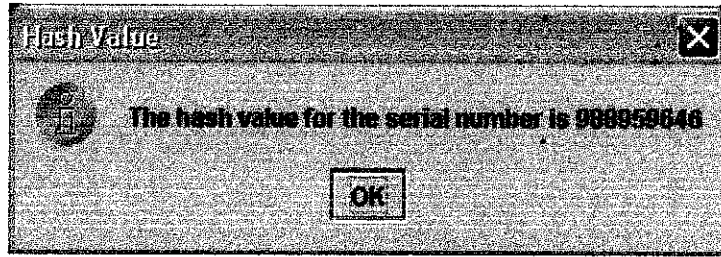


Figure 4.4



Figure 4.5

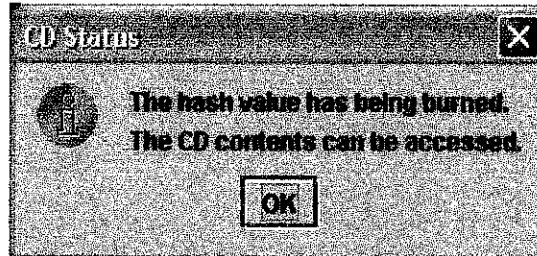


Figure 4.6

The next two part of the simulation demonstrates action taken by the CPU once the hash value has being detected.

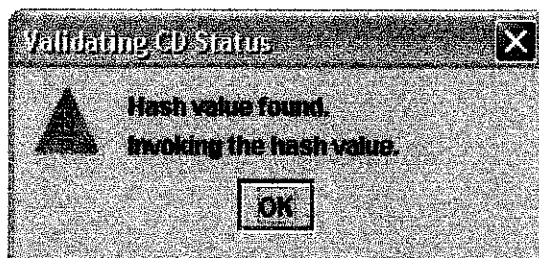


Figure 4.7

If the hash value of the CD does not match with the CPU, this screen will be shown.

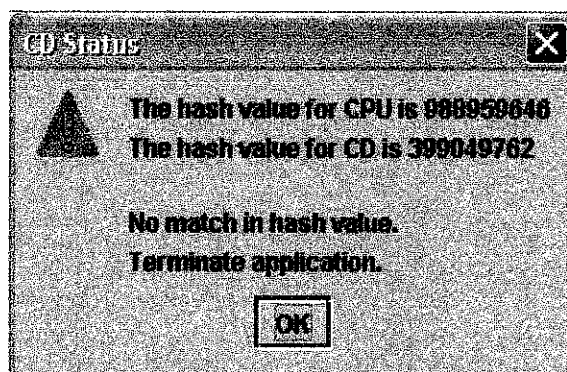


Figure 4.8

As if the hash value of CD matches with hash value of CPU, the status message will show as figure below;

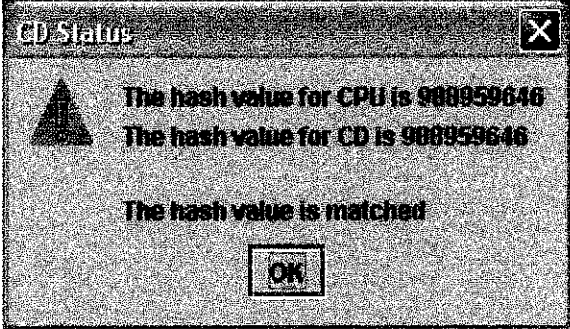


Figure 4.9

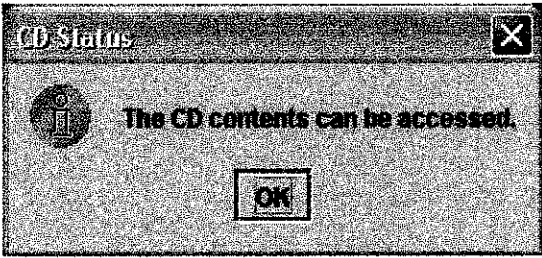


Figure 4.10

4.2. DISCUSSION

4.2.1. Copyright Protection

Copyright protection on CDs used to be rare, but as the popularity of CD recorders grew, so did the popularity of copy protection. A large percentage of games released in the past few years have been protected, same goes with the commercialized audio and software CDs.

Starting in 2000, music publishers started to sell some CDs with various copy protection schemes. A simple and commonly seen technique used in copyright protection of CDs is to increase the length of several files on the CD so that the length appears to be hundreds or megabytes long. This is accomplished by setting the files length in the disc image to be much larger than it really is. The file actually overlaps with many other files. As long as the application knows the true file length, the software will work fine. If the user tries to copy the files onto hard drive, or does a file-by-file disc copy, the attempt will fail because the CD will appear to hold a few GB of data. However, in practice, this technique does not foil pirates, because those pirates always do image copies. Moreover, none of the software standard provides a way to create such discs.

Another possible implementation is by giving sufficient control over the reader and mastering software to write faulty data into the ECC (Error Correcting Code) portion of a data sector. Standard CD hardware will automatically correct the “errors”, writing a different set of data onto the target disc. The reader then loads the entire sector as raw data, without doing any error correction. If it can’t find the original uncorrected data, it knows that it’s reading a “corrected” duplicate. However, this is only viable on systems like game consoles, where the drive mechanism and firmware are well defined. This can be defeated by using “raw” reads.

A less sophisticated and no longer effective method is to press a silver CD with data out beyond where a 74-minute CD can write. Copying the disc used to require hard-to-find CD-R blanks, but now it is easy to use an over-burned 80-minute disc.

Copy protection for early home computers such as the Apple II and Commodore 64 computers depended on precise knowledge of what exactly would happen if the hardware were forced to do something unusual such as to read a disk sector that was unformatted. Common method of copy protection for software is to write the software so that it requires some evidence from the user that they have actually purchased the software, usually by asking a question that only a user with a software manual could answer. However, this approach can be defeated by a user who has the patience to copy the manual with a photocopier, and it also suffers from BTO vulnerability.

Other software copy protection technique is by implementing a dongle, a piece of hardware containing an electronic serial number that must be plugged into the computer to run the software. This approach adds extra cost for the software publishers, therefore dongles are uncommon to be used and mostly found in high-end software packages costing several thousand dollars.

Copyright protection, on the whole, does not work. In general, if the disc can be read, then the contents can be copied. The success or failure of audio CD copyright protection depends upon two factors; how effective is it at preventing "casual copying", and what sort of problems do the legitimate owners of audio CDs encounter when playing the discs. A legitimate technical concern is that the copyright protection reduces the effectiveness of the error correction. Because some percentage of ECC is now required for proper playback on a 'clean' disc, the odds of scratches and fingerprints causing audible degradation are increased. In practice, if the static samples are relatively few and far between, the difference would be statistically insignificant.

4.2.2. Copyright Protection by Implementing TCPA

TCPA stands for Trusted Computing Platform Alliance, an initiative led by Intel. Their stated goal is a new computing platform for the next century that will provide for improved trust in the PC platform. TCPA provides a computing platform on which user cannot tamper with the application software, and where these applications can communicate securely with their authors and with each other. Trusted computing also will make it much harder for user to run unlicensed software.

How does the concept of TCPA can be implemented in copyright protection? TCPA provides for a monitoring and reporting component to be mounted in future PCs. The preferred implementation in the first phase of TCPA emphasized the role of a TCPA chip. The TCPA security subsystem is provided by hardware functions, called TPM (trusted platform module) function. The TPM includes five cryptographic functional units. It has a hardware random number generator (RNG), which provides a source of high-quality random numbers for on-chip key generation, as well as for application use. It has a hash unit and an associated hashing for message authentication calculator (HMAC). It also has the ability to generate hash keys of up to 2,048 bits on the chip, based on random numbers supplied by the RNG. Finally, it has an RSA that can perform signatures, encryption, and decryption. The TPM stores the important keys in non-volatile memory.

The serial number of the CPU will be created randomly on the chip at manufacture time and cannot be changed. This serial number will be considered as private key where it will never leaves the chip, while the public key (hash value of the serial number), is used for verification. TPM_CreateWrapKey generates a new hash key on the chip (public key), using the hardware RNG. A key must be typed as being either for signing or for encryption/decryption. The TPM does not allow a signature key to encrypt or an encryption key to sign, as this can lead to attacks. This public key will be stored in the

CD along with the Recorder Unique Identifier (RID). The RID is a 97-bit code recorded every 100 sectors. TPM_LoadKey command is used to load the key from the CD into one of the volatile key storage slots in the TPM. Later the TPM will check the key value of the CD whether it is matched or not with the private key stored in the chip. Therefore, it would be hard for user who does not have the right key to access the content of the CD. As it is hard to read the content, it will make it hard for user to copy it.

In order to enable the TPM, BIOS is responsible for starting up and clearing the TPM. At power-on, the TPM is activated but not started. The BIOS then must issue a TPM_Startup command. This command can do one or three things; deactivate the TPM, start up the TPM with a reset of the PCR (platform configuration register) or start up the TPM with a restore of PCR values from their saved states. If the BIOS deactivates the TPM, it remains deactivated until the next power cycle. A start up with clearing of the PCRs is done at boot time, so all PCR values are calculated correctly during boot. The TPM device driver is responsible for making a TPM_SaveState request at suspend time to ensure that valid PCR values are available at resume time.

CHAPTER 4

CONCLUSION AND RECOMMENDATION

5.1. Conclusion

Copyright infringement or piracy of commercial audio CDs and software has been increasing day by day. Piracy is a complicated topic which affects almost every aspect of our lives. What we decide to do about piracy as a society will determine our own cultural development or lack there of in the future. Therefore, it is important for public interest groups, technologists, and industry to work together to identify solutions in this complex technology and policy environment. Finding the corrective measure of preventing the piracy is worthwhile, not only for those in the creative industry itself, but for the society too. Wiping the piracy out should be the responsibility of every individual.

As referring to the result and discussion in the previous chapter, the research has achieved its stated objectives and aims. It is a worthwhile research as it enriches one's knowledge on this fast moving technology industry. The author has being introduced to the various techniques of CD copyright protection, the battle of music and software industry with the piracy and the TCPA framework.

5.2. Recommendation

As for the future recommendation, the author hopes that this concept will become into reality. This simulation should be applicable to be implemented in the future. With the current technologies and expertise, the author believe that this idea is achievable to be real. Hopefully, this future works are carried on with dedication and determination. Whatever it is done today is a transition to another step.

REFERENCES

Books

1. Uma Sekaran., 2003, "Research Methods for Business: A Skill Building Approach", Southern Illinois University, Carbondale, John Wiley & Sons
2. Ranjit Kumar, 1999, "Research Methodology: A Step-By-Step Guide for Beginners", London, Sage Publications
3. Anthony M. and Michael L., 2000, "Research Methods: A Process of Inquiry", State University of New York, Buffalo, Allyn and Bacon

Journals

4. Joseph Lowenstein, "The Author's Due : Printing and the Prehistory of Copyright", University of Chicago Press, 2002
5. D. Safford, "Clarifying Misinformation on TCPA", Oct 2002

Websites

6. <http://www.bsa.org>
7. <http://www.siia.net>
8. <http://en.wikipedia.org>
9. <http://www.developer.com>
10. <http://www.bambooweb.com>
11. <http://star-techcentral.com>
12. <http://www.trustedcomputing.org>

APPENDICES

Source Code for the Interface

```
import java.awt.*;
import java.awt.event.*;
import java.awt.Graphics.*;
import java.util.*;
import javax.swing.*;

public class Simulation extends JFrame {

    private JLabel statusLabel;
    private Color color = Color.lightGray;
    private Container container;

    //set up GUI
    public Simulation()
    {
        super("Simulation");

        JPanel northPanel = new JPanel();
        northPanel.setLayout(new BorderLayout());

        JPanel southPanel = new JPanel();
        southPanel.setLayout(new GridLayout(1,4));
        JButton button1 = new JButton("1st Simulation");

        button1.addActionListener(

            new ActionListener() {

                public void actionPerformed(ActionEvent event)
                {

                    GeneralHashFunctionLibrary ghi = new GeneralHashFunctionLibrary();
                    String key = "abcdefghijklmnopqrstuvwxyz1234567890";

                    //display the result

                    JOptionPane.showMessageDialog (
                        null, "CD is being inserted. \nChecking the hash value.\n", "My Disc (E:)",
```



```

JOptionPane.INFORMATION_MESSAGE);

JOptionPane.showMessageDialog (
    null, "No hash value found.\nCalculating hash value is in progress.\n", "Validating CD
Status",
    JOptionPane.WARNING_MESSAGE);

JOptionPane.showMessageDialog(
    null, "The hash value for the serial number is " + ghi.Hash(key), "Hash Value",
    JOptionPane.INFORMATION_MESSAGE);

JOptionPane.showMessageDialog(
    null, "Burning the hash value. \nPlease do not remove the CD.", "CD Status",
    JOptionPane.WARNING_MESSAGE);

JOptionPane.showMessageDialog(
    null, "The hash value has being burned.\nThe CD contents can be accessed.", "CD Status",
    JOptionPane.INFORMATION_MESSAGE);

    }
}
);
southPanel.add(button1);

JButton button2 = new JButton ("2nd Simulation");
button2.addActionListener(

    new ActionListener(){

        public void actionPerformed(ActionEvent event)
        {
            GeneralHashFunctionLibrary ghi = new GeneralHashFunctionLibrary();
            HashFunctionLibrary hfl = new HashFunctionLibrary();

            String key = "abcdefghijklmnopqrstuvwxy1234567890";
            long firstKey; //first serial number
            long secondKey; //second serial number
            String key1;
            String key2;

            //read in first serial number
            firstKey = ghi.Hash(key);

```

```

        //read in second serial number
        secondKey = hfl.Hash(key);

key1 = Long.toString(firstKey);
key2 = Long.toString(secondKey);

        //display the result

JOptionPane.showMessageDialog (
    null, "CD is being inserted. \nChecking the hash value.\n", "My Disc (E:)",
    JOptionPane.INFORMATION_MESSAGE);

JOptionPane.showMessageDialog (
    null, "Hash value found. \nInvoking the hash value.\n", "Validating CD Status",
    JOptionPane.WARNING_MESSAGE);

String output =

        "The hash value for CPU is " + ghl.Hash(key) +
        "\n\nThe hash value for CD is " + hfl.Hash(key);

if (key1.equals(key2))
    output += "\n\nThe hash value is matched";
else
    output += "\n\nNo match in hash value. \nTerminate application.";

JOptionPane.showMessageDialog(null, output, "CD Status",
    JOptionPane.WARNING_MESSAGE);

    }
}
);

southPanel.add(button2);

```

```

JButton button3 = new JButton("3rd Simulation");

button3.addActionListener(

new ActionListener(){

    public void actionPerformed(ActionEvent event)
    {
        GeneralHashFunctionLibrary ghi = new GeneralHashFunctionLibrary();

        String key = "abcdefghijklmnopqrstuvwxyz1234567890";
        long firstKey; //first serial number
        long secondKey; //second serial number
        String key1;
        String key2;

        //read in first serial number
        firstKey = ghi.Hash(key);

        //read in second serial number
        secondKey = ghi.Hash(key);

        key1 = Long.toString(firstKey);
        key2 = Long.toString(secondKey);

        //display the result

        JOptionPane.showMessageDialog (
            null, "CD is being inserted. \nChecking the hash value.\n", "My Disc (E:)",
            JOptionPane.INFORMATION_MESSAGE);

        JOptionPane.showMessageDialog (
            null, "Hash value found. \nInvoking the hash value.\n", "Validating CD Status",
            JOptionPane.WARNING_MESSAGE);

        String output =

            "The hash value for CPU is " + ghi.Hash(key) +
            "\nThe hash value for CD is " + ghi.Hash(key);
    }
}

```

```

        if (key1.equals(key2))
            output += "\n\nThe hash value is matched";
        else
            output += "\n\nNo match in hash value. \nTerminate application.";

        JOptionPane.showMessageDialog(null, output, "CD Status",
            JOptionPane.WARNING_MESSAGE);

        JOptionPane.showMessageDialog(
            null, "The CD contents can be accessed.", "CD Status",
            JOptionPane.INFORMATION_MESSAGE);

    }
}
);
southPanel.add(button3);

Container container = getContentPane();
container.add(northPanel, BorderLayout.NORTH);
container.add(southPanel, BorderLayout.SOUTH);
container.setBackground(Color.blue);

setSize(540, 300);
setVisible(true);

}

public void paint(Graphics g)
{
    //call superclass's paint method
    super.paint(g);
    g.setFont(new Font("Monospaced", Font.BOLD + Font.ITALIC, 28));
    g.setColor(Color.magenta);
    g.drawString("~~ Welcome ~~", 160,70);
    g.setFont(new Font("Monospaced", Font.BOLD + Font.ITALIC, 25));
    g.drawString("CD Copyright Protection Simulation", 20,110);
}
}

```

```
//execute application
public static void main(String args[])
{
    Simulation application = new Simulation();

    application.setDefaultCloseOperation(
        JFrame.EXIT_ON_CLOSE);
}

} //end of program
```

Source Code for Hash Function Algorithm

```
class GeneralHashFunctionLibrary
{
    public long RSHash(String str)
    {
        int b = 63689;
        int a = 38551;
        long hash = 0;
        for(int i = 0; i < str.length(); i++)
        {
            hash = hash * a + str.charAt(i);
            a = a * b;
        }
        return (hash & 0x7FFFFFFF);
    }
    /* End Of RS Hash Function */

    public long JSHash(String str)
    {
        long hash = 1315423911;

        for(int i = 0; i < str.length(); i++)
        {
            hash ^= ((hash << 5) + str.charAt(i) + (hash >> 2));
        }
        return (hash & 0x7FFFFFFF);
    }
    /* End Of JS Hash Function */

    public long PJWHash(String str)
    {
        long BitsInUnsignedInt = (long)(4 * 8);
        long ThreeQuarters = (long)((BitsInUnsignedInt * 3) / 4);
        long OneEighth = (long)(BitsInUnsignedInt / 8);
        long HighBits = (long)(0xFFFFFFFF) << (BitsInUnsignedInt - OneEighth);
        long hash = 0;
        long test = 0;
        for(int i = 0; i < str.length(); i++)
        {
            hash = (hash << OneEighth) + str.charAt(i);
            if((test = hash & HighBits) != 0)
```

```

        {
        hash = (( hash ^ (test >> ThreeQuarters)) & (~HighBits));
        }
    }
    return (hash & 0x7FFFFFFF);
}
/* End Of P. J. Weinberger Hash Function */

```

```

public long ELFHash(String str)
{
    long hash = 0;
    long x = 0;
    for(int i = 0; i < str.length(); i++)
    {
        hash = (hash << 4) + str.charAt(i);
        if((x = hash & 0xF000000L) != 0)
        {
            hash ^= (x >> 24);
            hash &= ~x;
        }
    }
    return (hash & 0x7FFFFFFF);
}
/* End Of ELF Hash Function */

```

```

public long BKDRHash(String str)

{
    long seed = 131; // 31 131 1313 13131 131313 etc..
    long hash = 0;
    for(int i = 0; i < str.length(); i++)
    {
        hash = (hash*seed)+str.charAt(i);
    }
    return (hash & 0x7FFFFFFF);
}
/* End Of BKDR Hash Function */

```

```

public long SDBMHash(String str)
{
    int hash = 0;
    for(int i = 0; i < str.length(); i++)
    {
        hash = str.charAt(i) + (hash << 6) + (hash << 16) - hash;
    }
    return (hash & 0x7FFFFFFF);
}
/* End Of SDBM Hash Function */

public long DJBHash(String str)
{
    int hash = 5381;
    for(int i = 0; i < str.length(); i++)
    {
        hash = ((hash << 5) + hash) + str.charAt(i);
    }
    return (hash & 0x7FFFFFFF);
}
/* End Of DJB Hash Function */

public long APHash(String str)
{
    int hash = 0;

    for(int i = 0; i < str.length(); i++)
    {
        if ((i & 1) == 0)
        {
            hash ^= ((hash << 7) ^ str.charAt(i) ^ (hash >> 3));
        }
        else
        {
            hash ^= (~((hash << 11) ^ str.charAt(i) ^ (hash >> 5)));
        }
    }
    return (hash & 0x7FFFFFFF);
}
/* End Of AP Hash Function */

} //end of the class

```